IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA, **-v-** **HO WAN KWOK, a/k/a "Miles Guo," "Miles Kwok," "Guo Wengui," "Brother Seven," or "The Principal,"** **and** **KIN MING JE, a/k/a "William Je,"** **and** **YANPING WANG, a/k/a "Yvette,"** **Defendants.**	Restitution of Seized Funds Criminal No.: 23-cr-118 (AT) **NOTICE OF SUPPLEMENTAL AUTHORITY COMPLETELY ALTERING THE GOVERNING LAW OF THIS CASE BY COUNSEL'S 6,540 CLIENTS** Assigned to the Honorable U.S. District Court Judge Analisa Torres, Presiding Judge

NOTICE OF SUPPLEMENTAL AUTHORITY COMPLETELY ALTERING THE GOVERNING LAW OF THIS CASE, FILED BY COUNSEL'S 6,540 CLIENTS [1]

Petitioners (Claimants) hereby file this NOTICE OF SUPPLEMENTAL AUTHORITY which as of 2:30 PM, July 18, 2023, ***COMPLETELY ALTERED THE GOVERNING LAW OF THIS CASE*** in every aspect of the crypto-currency activities of the Himalaya Exchange. The

[1] This most recent figure includes the original 3,345 customers authenticated by HEX (minus 72 who had dropped prior to our most recent April filing where we estimated the number of clients at 6,575). From this figure we have removed 35 clients who have dropped since April (21 of whom had been previously authenticated by the Himalaya Exchange (HEX)). This figure does not yet include additional sign-ups since our most recent April filing. This figure is a good faith estimate and not a final tally that will be finally reviewed and authenticated and matched with HEX compliance and account information.

law governing every aspect of this case touching on the crypto-currency, stable coin, or digital investments of the Himalaya Exchange (HEX) has been completely changed as of 3:30 PM July 18, 2025.

It should be noted that no aspect of this case is "FINAL" given that no "JUDGMENT" has been entered against Ho Wan Kwok (Miles Guo) or Kin Ming Je. Given that this case is not final, even as to the conviction of Kwok (Guo) without a Judgment having been entered, the case must now conform to the change in the governing law as of July 18, 2025.

From around 2:50 PM to 3:30 PM, EST, July 18, 2025, the President of the United States signed into law the informally named "GENIUS Act," designated as **"S.1582 — 119th Congress (2025-2026)."** It passed the U.S. Senate on June 17, 2025, and passed the U.S. House of Representatives on July 17, 2025 at about 3:53 PM.

It should be noted that even if the precise provisions of the new legislation might not be specifically "on point" with some aspect of this case, the overall approach to regulation and prosecution of digital assets is addressed by the "GENIUS Act." The methodology, policies, definitions of digital assets, definitions of terms, and goals of regulation and prosecution are all altered. Therefore, even where a detailed aspect of this case is not directly met by a provision of the Act, the overall policy and definitions still affect this case.

But more than that, the Chief Executive and the only law enforcement officer named and empowered in the U.S. Constitution, held a presentation, legal seminar, economic seminar, and policy session giving very strong, very clear, direction to the United States, Executive Branch, and by implication the U.S. Department of Justice and its representatives.

It would be difficult to listen to President Trump's 39 minute presentation and not interpret it as a powerful set of marching orders to the DOJ and the Executive Branch. Indeed

legal persecution of crypto currency was specifically targeted by Trump's remarks. And again, there is only one official identified in the U.S. Constitution as "the" law enforcement official of the United States of America – the President.

The President's signing session and explanation can be viewed on C-SPAN after the fact, as C-SPAN frequently preserves official sessions for later viewing.[2]

Furthermore, the U.S. Department of Justice on April 7, 2025, issued a "Memorandum for All Employees" from the Deputy Attorney General Todd Blanche titled "Ending Regulation by Prosecution" concerning the "digital assets industry." It should not be missed that this is a Memorandum "***for all Employees***" which means all representatives of the Department of Justice.

The directives given verbally by the President on July 18, 2025, and the enactment into law of the "Genius Act" must be viewed as confirming and giving more force to this Memorandum of April 7, 2025.

In general, the undersigned counsel is focused on the cancellation of the improper seizure and proposed forfeiture of the funds of his clients, who are an estimated 6,540 Members of (investors in) the Himalaya Exchange ("HEX"). HEX is based in the sovereign nation of the British Virgin Islands. Counsel's clients respectfully demand the return of their own investment funds (their personalty) which they entrusted to, invested with, or deposited in the Himalaya Exchange ("HEX") in their individually assigned HEX account. Those funds were illegally seized by the United States of America ("Government") which lacked jurisdiction over the extra-territorial entities associated with HEX.

[2] President Trump Signs Cryptocurrency Bill Into Law | Video | C-SPAN.org https://www.c-span.org/program/white-house-event/president-trump-signs-cryptocurrency-bill-into-law/662742

Also, to avoid any continuing confusion, the undersigned Counsel represents thousands of Members of HEX. There are thousands of Members whom Counsel does not represent, some of whom are represented by other attorneys or chose to represent themselves. The wording of Counsel's explanation should not be misunderstood to imply that all Members are represented by undersigned Counsel.

As Counsel has tried to clarify several times, he does not represent the criminal Defendants, and yet the seizure of his clients' funds are dependent upon the allegations against the criminal Defendants. So while undersigned Counsel and his clients might be legally agnostic (though interested on a human level) in the criminal prosecution itself, if the convictions against the Defendants, then there is no basis for seizing the funds of his client's investor clients or putting them through any procedure of any kind whatsoever. The money must simply be returned to my clients, immediately, and free of any of the unconscionable legal "waste" and "dissipation of assets" by the bonfire consuming my clients' funds by unnecessary processing, investigation, and delay.

Thus, Counsel is ethically required for his clients to zealously advocate for his clients that if the change of the law affects both the seizure of crypto-related assets and the existence of any crime supposedly justifying the seizure of my clients' funds these are reasons for his client's funds to be immediately returned to them. It is for other attorneys to argue for the Defendants. But if there never was any crime, then Counsel must point out that there is no reason to seize, waste, or dissipate his client's funds.

Also, of course, the prosecution has suggested (that is early on suspicioned) that as many as 80 different business entities may have been involved in the criminal Defendants' activities.

On further review of the case, access to case materials, and investigation, Counsel now

understands that the Himalaya Exchange subdivided its funds into 5-6 different business entities outside the United States all having a different functional goal supporting the Exchanges' business.

So, there are at least 74-75 business entities out of the Government's estimate of 80 that have nothing whatsoever to do with HEX and are unimpacted by revolutionary changes to cryptocurrency and cryptocurrency enforcement. These other 74 entities could very well have had business activities, offices, functions, etc. carried out within the territorial jurisdiction of the United States of America. Counsel has only limited information about these non-HEX activities.

So Counsel tries to clarify and emphasize that the other 75 non-HEX business entities may all have their own individual stories. They may be under U.S. jurisdiction. The activities relating to these 75 non-HEX entities may all come under different laws, certainly different fact patterns, all for different reasons. They may not receive the same benefits and deference that lawful crypto exchanges are now accorded.

Counsel is focusing only on HEX of the British Virgin Islands and its related companies outside the United States, etc.

Finally, counsel again objects and respectfully reminds the Court that his clients are by the explicit policies and requirements of HEX not subject to the jurisdiction of the United States Government. The Government has never responded to that problem except a half hearted "maybe" (not sure yet) from the personal Chapter 11 Trustee Luc Despins. The Court has not ruled on the lack of jurisdiction of the U.S. Government over HEX, its funds, or its Members / investors. But then again the U.S. Government has never responded in over a year and a half to these concerns and that was prior to the implementation of dramatic changes to how cryptocurrencies are treated. It seems reasonable to assume that there may be now additional

protections that apply to undersigned counsel's clients that do not apply to others, providing an additional reason to reverse the seizures.

It may be so unthinkable for professionals in New York City to believe that any investment company would not be eagerly seeking investments from Wall Street and throughout the United States, that nobody ever stopped to ask "But did HEX ever solicit any investments within the United States?" The hubris and status of Wall Street and the U.S. market would make that a question almost impossible to contemplate. Of course, everyone wants investments from within the United States! But with HEX, its creators emphatically rejected any participation of any U.S. citizen or resident or agent thereof. HEX, focused on a community of dissidents from the Chinese Communist Party, and distrustful of Western countries eager to please China, as well as wanting to avoid the onerous securities regulations decisively rejected and banned any investments from the United States and other countries including Japan. Whereas any resident of NYC would think it so obvious as to not require the question that everyone wants money invested from the USA, in fact HEX did not. And HEX prohibited any investments from the USA.

Trustee Luc Despins response of "maybe" effectively "I don't know, not sure yet" is not effective. Chapter 11 is created and authorized as a "reorganization" of an on-going business or businesses to restore a business or businesses to viability while paying off as many creditors as possible in the Chapter 11 plan. Federal law does not authorize Chapter 11 as a "liquidation."

A Chapter 7 bankruptcy petition is a "liquidation" aimed at collecting all available assets, selling them for the highest possible price, and distributing those funds among creditors according to legal hierarchies of status.

A Chapter 11 bankruptcy petition requires a plan and efforts to get a business back on its

feet and restore it to profitability and viability. The plan may have to recognize that all creditors cannot be made whole. Most commonly, the Chapter 11 plan distinguishes between different categories of creditors and attempts to make the higher priority creditors whole first. It may involve destroying the interests of shareholders (called a "cram down" [3]) if that promotes the ability to repay as many non-equity creditors as possible.

A Chapter 11 plan could fail. But Chapter 11 demands the creation and mapping out of a plan to get the business(es) back on its / their feet, and demands the actual attempt. If the plan fails then a "liquidation" may be required but not without first a good faith, diligent, sincere attempt to restore the business to viability. (It appears that modification of the line of business is a possibility so the nature, goals, and methods of the business could be altered to promote viability.)

Here, however, the Chapter 11 petition was filed by Ho Wan Kwok ***as an individual – not as a business or effectively in the name of any business.*** Later, Genevers was added as a co-petitioner but Counsel does not know why and Genevers appears to have nothing to do with HEX. If the addition of Genevers makes an actual business co-petitioner, it does not seem to have any relevance whatsoever to HEX.

Therefore, even Luc Despins' half-hearted, non-committal bookmark regarding extra-territorial jurisdiction is too vague, intentionally uncertain, and indeterminate to suffice.

---

[3] Cramdown of Equity in Chapter 11 Plan Requires Assessment of Equity's Value to Satisfy "Fair and Equitable" Standard, Business Restructuring Review (January 15, 2025). https://www.jonesday.com/en/insights/2025/01/cramdown-of-equity-in-chapter-11-plan-requires-assessment-of-equitys-value-to-satisfy-fair-and-equitable-standard

Humanitarian Concerns Over Conventional Forfeiture Procedures

If members of the Himalaya Exchange are forced to participate in conventional asset forfeiture processes, it would likely require them to submit identifying personal information to the U.S. government. This data exposure would effectively doxx members, many of whom are dissidents of the Chinese Communist Party (CCP). Given this population's legitimate fears of transnational repression, this risk presents the real possibility of triggering a humanitarian crisis. We have noticed the Government about this concern repeatedly from our first filing in ECF 186-1 page 18 and in Footnote 10 as co-victims of prior CCP data breaches:

> Many of the attorneys and staff assigned to this matter at the U.S. Attorney's office may sympathize with undersigned counsel's expressions of concern about information security since many of us (undersigned counsel as a former DOJ employee) have had had our clearance files compromised.[4] The Office of Personnel Management data breach was a 2015 data breach targeting Standard Form 86 (SF-86) U.S. government security clearance records retained by the United States Office of Personnel Management (OPM). One of the largest breaches of government data in U.S. history, the attack was carried out by an advanced persistent threat based in China, widely believed to be the Jiangsu State Security Department, a subsidiary of China's Ministry of State Security spy agency. Approximately 22.1 million records were affected, including records related to government employees, other people who had undergone background checks, and their friends and family. The breach included personally identifiable information such as Social Security numbers, as well as names, dates and places of birth, and addresses. State-sponsored hackers working on behalf of the Chinese government carried out the attack.
>
> In this matter it would be serious concern if Government ever were to consider it to be a good idea to obtain all account information from thousands of vulnerable Exchange customers who are located outside the United States requiring the Himalaya Exchange to unencrypt it and provide it to the US Government, when the US Government has a terrible track record of protecting such information.

[4] See Office of Personnel Management data breach - Wikipedia; Final notices going out this week to the 21 million people whose data was stolen in the security clearance breach - The Washington Post (December 8, 2015). https://www.washingtonpost.com/news/federal-eye/wp/2015/12/08/notifications-nearly-finished-in-security-clearance-files-breach/

Recent CCP hacking developments highlight this fear in neon lights:

Microsoft was revealed to have employed China-based engineers to support U.S. Department of Defense cloud services under a "digital escort" model. This practice drew condemnation from Secretary of Defense Pete Hegseth, who deemed it "obviously unacceptable." Microsoft responded by banning Chinese engineers from Pentagon projects.[5]

The issue is unlikely to be confined solely to the DoD, as Microsoft is a major cloud service provider for multiple U.S. government agencies through its Azure platform, which is authorized under the Federal Risk and Authorization Management Program (FedRAMP). The "digital escort" model, where U.S. citizens with security clearances oversee foreign engineers (including those in China) who provide technical support, was designed to meet federal contracting requirements for handling sensitive but unclassified data (Impact Levels 4 and 5). This model was critical to Microsoft securing government cloud contracts nearly a decade ago. Given that FedRAMP applies to cloud services across the federal government, similar arrangements could theoretically exist for other agencies, including the DoJ, which relies on

[5] Pete Hegseth Orders Review to Protect DOD Cloud Services From Chinese Hackers, ExecutiveGov (July 21, 2025). https://executivegov.com/articles/propublica-microsoft-china-engineers-dod-cloud-pete-hegseth

Microsoft to stop using China-based engineers for US military tech support, TechRadar (July 21, 2025). https://www.techradar.com/pro/security/microsoft-to-stop-using-china-based-engineers-for-us-military-tech-support

A Little-Known Microsoft Program Could Expose the Defense Department to Chinese Hackers, Propublica (July 15, 2025). https://www.propublica.org/article/microsoft-digital-escorts-pentagon-defense-department-china-hackers

Microsoft for cloud and IT services. The Probublica report noted that the "digital escort" system, where escorts often lack the technical expertise to properly oversee foreign engineers, could expose any federal system to cyberattacks, especially from a sophisticated actor like China. This suggests the problem could extend to other agencies, though no specific evidence confirms its use in the DoJ or elsewhere outside the DoD. The DoD's response, including Defense Secretary Pete Hegseth's two-week review of all Pentagon cloud contracts, indicates a focus on military systems, but it also hints at broader implications. Hegseth's statement that "some tech companies" use similar models suggests other providers (e.g., Amazon Web Services or Google Cloud) might face scrutiny, potentially affecting government-wide cloud services. While the available information does not explicitly confirm that the DoJ used China-based engineers in the same "digital escort" model, the DoJ's reliance on Microsoft Azure for cloud services raises the possibility of similar vulnerabilities. The DoJ handles sensitive data, including law enforcement records, criminal justice information, and national security-related investigations, which could be categorized as Impact Level 4 or 5 data, similar to the DoD's. A breach or backdoor in these systems could compromise any data my clients provide through the forfeiture process.[6]

In the trial of Ho Wan Kwok, it was proven that The Republic of China, governed by the CCP, embarked on a massive world-wide campaign to silence dissidents and critics of the CCP including within the United States of America. See, Trial Testimony, Paul Doran, July 4, 2024, Pages: 5085 – 5193; Trial Testimony of Jianhu Yi, July 3, 2024, pages 5040-5085.

[6] China-based hackers breached US government email accounts, Microsoft and White House say, CNN (July 12, 2023). https://www.cnn.com/2023/07/12/politics/china-based-hackers-us-government-email-intl-hnk/

This was also the subject of Stipulation 1 in the trial and following agreed stipulation was read to the jury on 29 May 2024:

MR. KAMARAJU: Okay. Your Honor, at this time the defense would like to read and enter into evidence a stipulation between the parties.
THE COURT: Go ahead.
MR. KAMARAJU: It's DX Stip 0001. And it reads:

"It is hereby stipulated and agreed by the United States of America and Miles Guo, the defendant, through their attorneys of record, that:

1. The FBI has investigated individuals who, working at the direction of the government of the People's Republic of China (the "PRC government") have engaged in an international campaign, known as "Operation Fox Hunt," to coerce individuals located in the United States and elsewhere to return to China to face charges brought by the PRC government or to otherwise reach financial settlements with the PRC government.

2. In 2017, a US law enforcement agency assessed that Mr. Miles Guo was the highest priority of China's repatriation efforts.

3. In 2017, a US law enforcement agency received information that Chinese officials were paying and providing food and signs to protestors of Mr. Guo.

4. In 2018, a US law enforcement agency received information that the PRC government had established a special investigative group in China to manage China's investigation of, and actions against, Mr. Guo.

5. To carry out some of the objectives of Fox Hunt, in 2017, the PRC government tasked a specially designated group of operatives ("the Group") with discrediting and harassing individuals, including Mr. Guo, by using interactive computer

services and electronic communication systems. The Group is based out of the Beijing Municipal Public Security Bureau at a facility in Beijing's Dong Cheng District. The Group was previously referred to as the "Cyber Investigation Team" and was later referred to as the 9112 Special Project Working Group. The Group's tactics aimed at Mr. Guo included using anonymized social media accounts operated by the Group and by pressuring US social media companies to remove Mr. Guo and US-based associates of Mr. Guo from social media platforms. These efforts were part of the PRC government's broader effort to prevent, disrupt, and harass Mr. Guo's use of social media and other online platforms to disseminate and discuss disfavored content. In or about December 2018, officers of the Group were directed to post three videos or posts daily with YouTube and Facebook accounts, with one of the posts required to be anti-Mr. Guo. On February 3, 2020, a PRC government official issued a tasking requirement that every member of the Group shall write an original article with content related to targeting Mr. Guo, the COVID pandemic, or Hong Kong. The FBI investigated the Group's activities, including its activities aimed at Mr. Guo, and the US government has charged many of the Group's members with violations of US law.

6. Since Mr. Guo fled the PRC, the PRC government has sought his return for prosecution in the PRC and has employed numerous methods to effect Mr. Guo's capture or arrest. In May 2017, the PRC government sent four undeclared agents from the PRC's Ministry of State Security ("MSS") to the United States to attempt to cause Mr. Guo's coerced repatriation to the PRC as part of the Fox Hunt initiative. The US government disrupted the PRC government's efforts to forcefully repatriate Mr. Guo and Mr. Guo continued to reside in the United States.

* * *

THE COURT: It is admitted.

Moreover, the Republic of China ("China") seems to have set up a systematic enforcement network of fake police stations within the United States in order to terrorize and persecute refugees from Chinese communism and other critics.

The Boston case is hardly an exception. Last month, the Department of Justice indicted two New York residents, Lu Jianwang and Chen Jinping, for "conspiring to act as agents" of the CCP's Ministry of Public Security (MPS) and for obstructing justice by destroying evidence of their communications with the MPS. The two were operating an MPS secret police station in Manhattan's Chinatown neighborhood, which was aiding the CCP's transnational repression by intimidating and threatening Chinese dissidents.[7]

The revelation that Microsoft employed China-based engineers under a "digital escort" model to support sensitive U.S. government cloud systems—condemned by Defense Secretary Pete Hegseth as "obviously unacceptable"—not only raises alarming cybersecurity concerns about the Pentagon and other agencies like the DOJ that rely on Microsoft's FedRAMP-authorized services, but also underscores the broader national security threat posed by the CCP's transnational repression campaigns, including Operation Fox Hunt, covert propaganda operations and illegal police stations on U.S. soil targeting Chinese dissidents. Forcing HEX members into forfeiture proceedings designed prior to the emergence of stable coin exchanges overseas with overseas customers who remain at risk of retaliation, may invite similar exposure and potentially ***catastrophic*** consequences. The government would do well to consider the GENIUS Act's mandates and align enforcement with both the law and humanitarian principles and return funds

[7] Erin Walsh and Andrew Harding, "Crack Down on Illegal Chinese Police Stations in the US," The Hill (May 18, 2023). https://thehill.com/opinion/national-security/4008817-crack-down-on-illegal-chinese-police-stations-in-the-u-s/

to HEX or at least through HEX where doxxing transfers to unsecure systems are not required and funds can be returned without inadvertent disclosures through facilitation by HEX using its secure, military-grade encryption systems

Conclusion

Given the clear changes in law and Executive Branch policy, coupled with the potential for extreme harm, there is no legal or ethical basis for requiring the continued seizure, wasting, or forced processing of Petitioners' funds through a doxxing process. As stated in prior filings, the forfeitures should be reversed *in toto* on jurisdictional grounds. In the event the GENIUS Act does not differentiate overseas funds held in custodial accounts for the HEX exchange—which were established through heavily counseled legal structuring to avoid jurisdictional claims by the U.S. government—these funds should be returned immediately through the HEX system, which does not require disclosure of sensitive financial data. Ideally, the Government would make a joint motion to accept a consolidated filing on behalf of undersigned counsel’s clients, establishing a clearance process that provides the Government full access in a secure environment without the necessity of transferring data to insecure government systems. This

would be free from any administrative delays or legal gamesmanship. The Claimants' requests for the Court to rule the entire case lacking in jurisdiction with regard to HEX remain pending.

Dated: July 28, 2025

RESPECTFULLY SUBMITTED

/s/ Brad Geyer
Bradford L. Geyer, PHV
NJ 022751991
Suite 141 Route 130 S. 303
Cinnaminson, NJ 08077
Brad@FormerFedsGroup.Com
(856) 607-5708

CERTIFICATE OF SERVICE

I hereby certify that on July 28, 2025, a true and accurate copy of the forgoing was electronically filed and served through the ECF system of the U.S. District Court for the Southern District of New York.

/s/ Brad Geyer
Bradford L. Geyer, PHV
NJ 022751991
Suite 141 Route 130 S. 303
Cinnaminson, NJ 08077
Brad@FormerFedsGroup.Com
(856) 607-5708